Amendments to the Specification:

*Please amend paragraph [0001] as follows:

[0001] This application is a continuation-in-part of U.S. Application No. 09/853,835, entitled "Digital Watermarking Apparatus, Systems and Methods," filed May 10, 2001 (published as US 2002-0169721 A1). This application is related to U.S. Patent Application Nos. 09/562,049, filed May 1, 2000, and 09/790,322, filed February 21, 2001 (published as US 2001-0037313 A1). This application is also related to PCT Application No. PCT/US 01/14014 (published as WO 01/84438), filed in the United States Receiving Office on April 30, 2001, entitled "Digital Watermarking Systems."

*Please amend paragraph [0012] as follows:

[0012] Digital watermarking systems typically have two primary components: an embedding component that embeds the watermark in the media content, and a reading component that detects and reads the embedded watermark. The embedding component embeds a watermark pattern by altering data samples of the media content. The reading component analyzes content to detect whether a watermark pattern is present. In applications where the watermark encodes information, the reading component extracts this information from the detected watermark. Commonly assigned U.S. Application No. 09/503,881, filed February 14, 2000 (published as U.S. Patent No. 6,614,914), discloses various encoding and decoding techniques. United States Patent No. 5,862,260 discloses still others. Of course, artisans know many other watermark techniques that may be suitably interchanged with the present invention.

*Please amend paragraph [0025] as follows:

[0025] Terminal 16 preferably includes a general purpose or dedicated computer, incorporating electronic processing circuitry (e.g., a processor), memory (e.g., RAM, ROM, magnetic and/or optical memory, etc.), an interface to the input device 14, a display screen or other output device, and a network connection. The network connection can be used to connect to a network 22, such as an intranet, internet, LAN, WAN, wireless network, or other such network, to communicate with at least computers 18 and 20. (Of course, terminal 16 may be a handheld computing device, instead of the computing terminal shown in Fig. 1, such as is disclosed in assignee's U.S. Patent Application No. 09/842,282, filed April 24, 2001, published as US 2002-0006212 A1.).

*Please amend paragraph [0033] as follows:

[0033] Further aspects of the present invention are now disclosed. With reference to Figures 1 and 3, a digitally watermarked document 12 is presented to input device 14 (step S1, Fig. 3). The input device 14 captures an image(s) of the document and conveys such to terminal 16. Executing watermark decoding software instructions (e.g., a "decoder"), terminal 16 decodes the digital watermark embedded within the captured image data and recovers the watermark identifier (step S2). Of course, the decoder may be integrated into various software applications, operating system, web browser, independent software module, device, system, etc. Such a decoder detects and reads an embedded watermark (or watermarks) from a signal suspected of containing the watermark. In one embodiment, the decoder includes Digimarc MediaBridge software, available at www.digimarc.com or through Digimarc Corporation, headquartered in Beaverton, ~~Tualatin,~~ Oregon, U.S.A. Of course, other watermark decoding software may be used in other embodiments.

*Please amend paragraph [0062] as follows:

[0062] Returning to Figure 12, server 20 identifies a validation key (step S80). In step 82, server 20 queries the validation key database to determine whether the validation key has been previously received (or received within a predetermined time period). If the validation key is not stored in the database (or has not been received within a predetermined period), access to the website is denied (step S84). Otherwise access to the website is allowed (S86). Of course the validation checking method illustrated in Figure 12 could be combined with the methods illustrated in Figures 10 and/or 11. Such a system helps to prevent copy attacks again the system.